[translation]

(19) KOREAN INTELLECTUAL PROPERTY OFFICE (KR)

(12) KOREAN PATENT LAID-OPEN PUBLICATION (A)

(51) Int. Cl.[6]
G06F 17/60 (early disclosure)

(11) Laid-Open Publication No.: 2000-0024217
(43) Laid-Open Publication Date: May 6, 2000

(21) Application No.: 2000-0004492
(22) Filing Date: January 29, 2000

(71) Applicant: Seung-Wook Jang

(72) Inventor: Seung-Wook Jang

(54) Title: AN AUTHENTICATION SYSTEM FOR ELECTRONIC COMMERCE IN DATA CENTER AND AN METHOD FOR PROVIDING AUTHENTICATION SERVICE

ABSTRACT

The present invention relates to an authentication system for electronic commerce in a data center. Such authentication system in the authentication system dispersed in unit of a data center unit including at least one electronic commerce-relevant enterpriser and electronic commerce authentication authority comprises:
a server of an electronic commerce authentication authority issuing certificates to electronic commerce enterprisers; and
a server of an electronic commerce enterpriser setting a security channel with a terminal device of a purchaser based on said issued server certificate and a session key generated in the purchaser's terminal device, and requesting registration of the electronic commerce authentication service under agreement of the purchaser in a process of client registration and renewal application of the purchaser,
wherein said electronic commerce authentication authority server generates a private key and a public key of the purchaser in pairs for electronic signature by request of the purchaser, transmits the private key for the electronic signature of the purchaser, issues and stores the certificate to the purchase, and enables the purchaser to store the certificates in the terminal device by sending a password that can decrypt the encrypted private key for the electronic signature of the purchaser to an electronic mail address which the purchaser designates at the registration application

Brief description of the drawings

Fig. 1 roughly illustrates a system of an electronic commerce authentication service of a data center in accordance with the present invention.

Fig. 2 illustrates a specific embodiment of the electronic commerce authentication system of the data center in accordance with the present invention.

Claims

1. An authentication system for electronic commerce in a data center, comprising:
a server of an electronic commerce authentication authority issuing certificates to electronic commerce enterprisers; and
a server of an electronic commerce enterpriser setting a security channel with a terminal device of a purchaser based on said issued server certificate and a session key generated in the purchaser's terminal device, and requesting registration of the electronic commerce authentication service under agreement of the purchaser in a procedure of client registration and renewal application of the purchaser,
wherein said electronic commerce authentication authority server generates a private key and a public key of the purchaser in pairs for an electronic signature according to the request of the purchaser, transmits an encrypted private key for the electronic signature of the purchaser, issues the certificate to the purchaser and stores it, and enables the purchaser to store the certificates in the terminal device by sending a password that can decrypt the encrypted private key for the electronic signature of the purchaser to a electronic mail address which the purchaser designates during the registration application in the authentication system distributed by a data center unit including at least one electronic commerce enterpriser and electronic commerce authentication authority.

2. The authentication system for electronic commerce in a data center of claim 1,
wherein when the electronic commerce occurs between certain electronic commerce

enterprisers inside/outside the data center issued with the server certificates of said purchaser and said electronic commerce authentication authority,

wherein said electronic commerce enterpriser server is programmed to request the confirmation of the electronically signed purchase application by said purchaser to the server of said electronic commerce authentication authority after the electronic commerce enterpriser electrically signed, and

wherein said electronic commerce authentication authority server searches a directory server dispersedly constructed in unit of a data center, checks validity of the certificates of the purchaser and the electronic commerce enterpriser, is programmed to issue the confirmation regarding an occurrence and the breakdown of the transaction of said purchaser and electronic commerce enterpriser after the electronic signature of the authority, and based on this, is programmed to proceed the relevant processes such as charge, request, intermediation, distribution, etc., connected with the electronic commerce.

3. The authentication system for electronic commerce in a data center of Claim 1, wherein said server of the electronic commerce enterpriser comprises:

a means for applying the authentication registration setting a purchaser's terminal device and a security based on the server certificate issued from said electronic commerce authentication authority and performing the authentication service registration application as a proxy under the purchaser's permission in the client registration and renewal application of the purchaser; and

a means for requesting a transaction confirmation requesting the confirmation of the purchase application of the electronic commerce to the electronic commerce authentication authority after the electronic signature by the private key of the electronic commerce enterpriser regarding the purchaser information electrically signed by the private key for electric signature of the purchaser when the electronic commerce occurs between said electronic commerce enterpriser and the purchaser.

4. The authentication system for electronic commerce in a data center of claim 1, wherein said server of the electronic commerce authentication authority comprises:

a means for issuing a certificate for issuing the certificate to the server of said electronic commerce enterpriser according to a predetermined procedure;

a means for generating a private key and a public key for electronic signature of the purchaser in pairs according to the registration application at the server of said electronic commerce authentication authority;

a means for managing a directory storing and managing said certificate and distributing and constructing the certificate based on a relative subscriber path when commerce confirmation of the electronic commerce unit is requested;

a means for checking the validity of the certificate by searching the directory dispersedly constructed based on the relative subscriber path and sending the confirmation to the purchaser and the electronic commerce enterpriser when the transaction confirmation of said electronic commerce unit is requested;

a means for connecting additional services checking the validity of the certificates of said purchaser and electronic commerce enterpriser by searching the directory server dispersedly constructed in unit of a data center at the server of said electronic commerce authentication authority, issuing the confirmation regarding an occurrence and a breakdown of the transaction to the purchaser and the electronic commerce enterpriser after the electronic signature of the electronic authentication authority, and proceeding the relevant procedure, such as charge, request, intermediation, distribution, etc., connected with the electronic commerce.

5. The authentication system for electronic commerce in a data center of claim 4, wherein said means for issuing the certificate performs the function of transmitting the private key for electronic signature of the purchaser generated at said server of the electronic commerce authentication authority and sending a password that can decrypt the encrypted private key to an electronic mail address wherein the purchaser designates at the time of the registration application.

6. A method of providing authentication service for electronic commerce in a data center which is dispersedly constructed in unit thereof, comprising the steps of:

(a) setting the security channel between said electronic commerce enterpriser server and said purchaser's terminal device based on the session key generated in the purchaser's terminal device connected to the electronic commerce enterpriser server;

(b) applying the authentication service registration to the electronic commerce authentication authority upon the purchaser's permission in the process of client registration and renewal process of the purchaser by said electronic commerce enterpriser;

(c) generating the private key and the public key for electronic signature of the purchaser in pairs by said electronic commerce authentication authority according to the authentication service registration application of said purchaser, transmitting the encrypted private key for electronic signature of the generated subscriber to the purchaser, issuing and storing the certificate of the purchaser, and transmitting the password that can decrypts the private key for electronic signature of the encrypted purchaser to the electronic mail address designated when the purchaser registers the authentication service, etc.;

(d) storing the private key of the encrypted electronic signature of the purchaser transmitted from the electronic commerce authentication authority to said purchaser's terminal device, decrypting the password sent to the designated electronic mail address, and storing it in the purchaser's terminal device;

(e) transmitting an order breakdown of a transaction to said electronic commerce authentication authority server after the purchaser's signature, when the electronic commerce occurs between the purchaser issued with the certificate from said electronic commerce authentication authority and an optional electronic commerce enterpriser issued with the server certificate of the electronic commerce authentication authority inside/outside the data center;

(f) requesting a confirmation to the electronic commerce authentication authority after the electronic signature regarding the order breakdown transmitted from said purchaser's terminal device by said electronic commerce enterpriser;

(g) searching the directory server dispersedly constructed in unit of a data server, checking the validity of the certificate of the purchaser and the electronic commerce enterpriser, and transmitting the confirmation to said purchaser's terminal device and the electronic commerce enterpriser after the electronic signature of the electronic authentication authority by said electronic commerce authentication authority; and

(h) proceeding the relevant procedure such as charge, request, intermediation, distribution, etc. connected with the electronic commerce based on the confirmation of the server of said electronic commerce authentication authority.

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.
G06F 17/60(조기공개)

(11) 공개번호 특2000-0024217
(43) 공개일자 2000년05월06일

(21) 출원번호 10-2000-0004492
(22) 출원일자 2000년01월29일

(71) 출원인 장승욱
서울특별시 광진구 군자동 352-8

(72) 발명자 장승욱
서울특별시 광진구 군자동 352-8

(74) 대리인 이영필, 권석흠, 이상용

심사청구 : 없음

(54) 데이터 센터의 전자거래 인증시스템 및 인증서비스 제공방법

요약

본 발명은 데이터 센터의 전자거래 인증시스템에 관한 것으로, 이러한 인증시스템은 적어도 하나의 전자거래관련사업자와 전자거래인증기관을 포함하는 데이터센터 단위로 분산된 인증시스템에 있어서, 상기 전자상거래관련사업자에 인증서를 발급하는 전자거래인증기관 서버; 및 상기 발급 받은 서버인증서와 구매자 단말장치에서 생성한 세션키를 근간으로 구매자 단말장치와의 보안채널을 설정하고, 구매자의 고객등록 및 갱신신청 처리과정에서 구매자의 동의하에 전자거래인증서비스 등록을 신청하는 전자거래관련사업자 서버를 포함하고, 상기 전자거래인증기관 서버는 구매자의 신청에 따라 구매자의 전자서명용 비밀키, 공개키쌍을 생성하고 구매자의 전자서명용 비밀키를 암호화하여 전송하고, 구매자에게 인증서를 발급 및 저장하고, 암호화된 구매자의 전자서명용 비밀키를 복호화할 수 있는 비밀번호를 구매자가 등록신청시 지정한 전자우편주소로 발신하여 구매자가 단말장치에 인증서를 저장할 수 있게 함을 특징으로 한다.

대표도

도2

명세서

도면의 간단한 설명

도 1은 본 발명에 의한 데이터 센터의 전자거래 인증서비스에 대한 개략적인 시스템을 도시한 것이다.

도 2는 본 발명에 의한 데이터 센터의 전자거래 인증시스템의 구체적인 실시예를 도시한 것이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 전자거래시스템에 관한 것으로, 더욱 상세하게는 전자거래의 안전성 및 신뢰성 보장을 위하여 전자거래에서 구매자 및 판매자에게 비밀성, 무결성, 부인방지, 신원확인 등 인증서비스의 기본적 기능을 제공하고, 구매자 및 판매자의 편의를 증진한 인증서 발급 및 처리 절차의 개발하며, 전자거래시장의 물리적 중심기능을 담당하는 데이터센터 단위로 인증 및 디렉토리서버를 분산함으로써 최적화된 인증시스템의 구축 및 운용에 관한 기술이다.

기존의 전자거래시장에서 본 발명에 관련한 종래 기술을 찾는다면 SET 정도가 있을 수 있다.

발명이 이루고자 하는 기술적 과제

본 발명이 이루고자하는 기술적 과제는 전자거래의 안전성 및 신뢰성 보장을 위하여 전자거래단위에서 구매자 및 판매자에게 비밀성, 무결성, 부인방지, 신원확인 등 인증서비스의 기본적인 기능을 제공하고, 전자거래시장에서 인증서비스의 보급을 목적으로 인증서비스의 등록 및 이용절차를 단순화하여 구매자 및 판매자의 편의를 증진하고, 인증서비스의 근간인 PKI(Public Key Infrastructure)의 구축을 용이하게 하기 위해 가상적인 전자거래시장의 물리적 중심기능을 담당하는 각각의 데이터센터 단위로 인증 및 디렉토리 서버를 분산 구축하고 상호 연동하게 함으로써 인증서의 운용관리를 효율적으로 할 수 있는 데이터 센터 중심의 전자거래 인증시스템 및 인증서비스 제공 방법을 제공함에 있다.

발명의 구성 및 작용

상기 기술적과제를 해결하기 위한 본 발명에 의한 데이터 센터의 전자거래 인증시스템은 적어도 하나의 전자거래관련사업자와 전자거래인증기관을 포함하는 데이터센터 단위로 분산된 인증시스템에 있어서, 상기 전자상거래관련사업자에 인증서를 발급하는 전자거래인증기관 서버; 및 상기 발급 받은 서버인증서와 구매자 단말장치에서 생성한 세션키를 근간으로 구매자 단말장치와의 보안채널을 설정하고, 구매자의 고객등록 및 갱신신청 처리과정에서 구매자의 동의하에 전자거래인증서비스 등록을 신청하는 전자거래관련사업자 서버를 포함하고, 상기 전자거래인증기관 서버는 구매자의 신청에 따라 구매자의 전자서명용 비밀키·공개키쌍을 생성하고 구매자의 전자서명용 비밀키를 암호화하여 전송하고, 구매자에게 인증서를 발급 및 저장하고, 암호화된 구매자의 전자서명용 비밀키를 복호화할 수 있는 비밀번호를 구매자가 등록신청시 지정한 전자우편주소로 발신하여 구매자가 단말장치에 인증서를 저장할 수 있게 함을 특징으로 한다.

또한, 상기 구매자와 상기 전자거래인증기관의 서버인증서를 발급받은 데이터센터내·외의 임의의 전자거래관련사업자간의 전자거래 발생시, 상기 전자거래관련사업자 서버는 상기 구매자가 전자서명한 구매신청에 대한 확인을 전자거래사업자의 전자서명 후, 상기 전자거래인증기관의 서버에 요청하도록 프로그램되고, 상기 전자거래인증기관 서버는 데이터센터단위로 분산구축된 디렉토리서버를 검색하여 구매자 및 전자거래관련사업자 인증서의 유효성을 확인하고 인증기관의 전자서명 후, 상기 구매자 및 전자거래관련사업자의 거래발생 및 거래내역에 대한 확인서를 발급하도록 프로그램되고, 이를 근거로 전자거래와 연계된 과금, 청구, 중개, 물류 등의 관련절차를 진행할 수 있게 하는 프로그램됨을 특징으로 한다.

또한, 상기 전자거래관련사업자 서버는 상기 전자거래인증기관 서버로부터 발급받은 서버인증서를 근간으로 구매자 단말장치와 보안채널을 설정하고, 구매자의 고객등록 및 갱신신청 과정에서 구매자의 동의를 얻어 전자거래 인증서비스 등록신청을 대행하는 인증등록신청수단; 및 상기 전자거래관련사업자가 구매자와의 전자거래 발생시, 구매자의 전자서명용 비밀키로 전자서명된 구매정보에 대하여 전자거래관련사업자의 비밀키로 전자서명 후, 전자거래인증기관에 전자거래의 구매신청의 확인을 요청하는 거래확인신청수단을 포함함을 특징으로 한다.

또한, 상기 전자거래인증기관의 서버는 상기 전자거래관련사업자의 서버에 소정의 절차에 따라 인증서를 발급하는 인증서 발급수단; 상기 전자거래인증기관의 서버에서 등록신청에 따라 구매자의 전자서명용 비밀키, 공개키쌍을 생성하는 키 쌍 생성수단; 상기 인증서를 저장 및 관리하고, 전자거래 단위의 거래 확인요청시 상대적인 가입자 경로를 기준으로 분산 구축하는 디렉토리관리수단; 상기 전자거래 단위의 거래 확인요청시 상대적인 가입자 경로를 기준으로 분산 구축된 디렉토리를 검색하여 인증서의 유효성을 확인하고 구매자 및 전자거래관련사업자에게 확인서를 발신하는 전자거래확인수단; 상기 전자거래인증기관의 서버에서 데이터센터 단위로 분산구축된 디렉토리서버를 검색하여 상기 구매자 및 전자거래관련사업자 인증서의 유효성을 확인하고 전자거래인증기관의 전자서명 후, 구매자 및 전자거래관련사업자에게 거래발생 및 거래내역에 대한 확인서를 발급하고, 이를 근거로 전자거래와 연계된 과금, 청구, 중개, 물류 등의 관련 절차를 진행하는 부가서비스연동수단; 및 상기 전자거래 단위의 인증서비스 제공을 위하여 데이터 센터 단위로 분산구축된 인증시스템간에 연동하는 인증서비스연동수단을 포함함을 특징으로 한다.

또한, 상기 인증서발급수단은 상기 전자거래인증기관의 서버에서 생성된 구매자의 전자서명용 비밀키를 암호화하여 전송하고 암호화된 비밀키를 복호화 할 수 있는 비밀번호를 인증서비스 등록시 지정한 전자우편주소로 발신하는 기능을 수행함을 특징으로 한다.

상기 다른 기술적 과제를 해결하기 위한 본 발명에 의한 데이터 센터의 전자거래의 인증서비스 제공 방법은 (a)전자거래관련사업자 서버에 접속한 구매자 단말장치에서 생성한 세션키를 근간으로 상기 전자거래관련사업자 서버와 상기 구매자 단말장치간의 보안채널을 설정하는 단계; (b)상기 전자거래관련사업자 서버가 구매자의 고객등록 및 갱신 처리과정에서 구매자의 동의를 얻어 전자거래인증기관에 인증서비스 등록을 신청하는 단계; (c)상기 구매자의 인증서비스 등록신청에 따라 상기 전자거래인증기관 서버는 구매자의 전자서명용 비밀키·공개키 쌍을 생성하고, 생성된 가입자의 전자서명용 비밀키는 암호화하여 구매자에게 전송하며, 구매자의 인증서를 발급 및 저장하고, 암호화된 구매자의 전자서명용 비밀키를 복호화할 수 있는 비밀번호를 구매자가 인증서비스 등록시 지정한 전자우편주소로 전송하는 단계; (d)상기 구매자 단말장치에 전자거래인증기관 서버로부터 전송된 구매자의 암호화된 전자서명 비밀키를 저장하며, 지정한 전자우편주소로 발신된 비밀번호를 복호화하고 구매자의 단말장치내에 저장하는 단계; (e)상기 전자거래인증기관 서버로부터 인증서를 발급받은 구매자와 데이터센터내·외의 전자거래인증기관의 서버인증서를 발급받은 임의의 전자거래관련사업자간의 전자거래발생시, 구매자의 전자서명 후 상기 전자거래관련사업자 서버에 주문내역을 전송하는 단계; (f)상기 전자거래관련사업자 서버는 상기 구매자 단말장치로부터 전송된 주문내역에 대하여 전자서명 후, 전자거래인증기관 서버에 확인을 요청하는 단계; (g)상기 전자거래인증기관 서버는 데이터센터 단위로 분산구축된 디렉토리서버를 검색하여 구매자 및 전자거래관련사업자 인증서의 유효성을 확인하고 전자거래인증기관의 전자서명 후, 상기 구매자 단말장치 및 전자거래관련사업자 서버에 확인서를 전송하는 단계; 및 (h)상기 전자거래인증기관 서버의 확인을 근간으로 전자거래와 연계된 과금, 청구, 중개, 물류 등의 관련절차를 진행하는 단계를 포함함을 특징으로 한다.

이하 도면을 참조하여 본 발명을 상세히 설명하기로 한다.

본 발명은 전자거래가 발생하는 가상공간에서 네트워크의 물리적 허브 기능을 담당하는 데이터센터 단위로 인증 및 디렉토리서버를 분산 구축하고 이들의 연동을 위한 백본을 구성하여 효과적인 전자거래 단위의 인증서비스 제공을 가능하게 하며 인증서비스의 PKI구축에 용이한 계층적 하부구조를 가져갈 수 있게 한다.

도 1은 데이터센터 중심의 인증서비스에 대한 개략적인 시스템을 도시한 것이다.

도 1은 데이터센터 단위로 인증시스템을 분산구축하여 전자거래관련사업자의 서버에 인증서를 발급하고, 전자거래관련사업자를 일반에 대한 인증서비스 등록기관화하여 PKI를 구축하고, B2C 및 B2B간의 전자거래 단위에 있어 인증서비스를 제공하는 시스템을 도시한 것이다.

즉, 데이터센터내 전자거래관련사업자의 서비스 가입자는 전자거래인증기관의 인증서비스 고객으로 등록되고, 등록된 고객은 상기 인증기관으로부터 인증서를 발급받은 임의의 전자거래관련사업자간의 전자거래에 있어서도 동일한 인증서비스를 제공받을 수 있으며, 전자거래관련사업자는 인증서비스의 PKI에 등록된 임의의 구매자를 대상으로 안전성 및 신뢰성이 보장되는 전자거래를 할 수 있게 된다.

도 2는 본 발명에 의한 데이터 센터의 전자거래 인증시스템의 구체적인 실시예를 도시한 것으로, 구매자 단말장치(210), 전자거래관련사업자 서버(220) 및 전자거래인증기관 서버(230)로 이루어진다.

구매자 단말장치(210)는 전자거래인증기관 서버(230)로부터 전송된 전자서명용 구매자 비밀키를 저장하고, 전자거래인증기관 서버(230)으로부터 전자우편을 통하여 수신된 비밀번호를 이용하여 구매자 전자서명용 비밀키를 복호화하고 구매자의 인증서를 저장한다.

전자거래관련사업자 서버(220)는 구매자 단말장치(210)로부터 전자거래를 위한 고객 등록 및 갱신 신청을 받아 전자거래인증기관에 구매자의 전자서명용 비밀키, 공개키 쌍의 생성 및 인증서 발급을 요청하는 인증등록신청수단(222) 및 상기 절차에 따라 인증서를 발급받은 구매자와의 전자거래 발생시의 거래확인신청수단(221)을 구비한다.

인증등록신청수단(222)은 전자거래인증기관으로부터 발급받은 서버인증서를 근간으로 구매자 단말장치(210)와 보안채널을 설정하고, 구매자의 고객등록 및 갱신신청 과정에서 구매자의 동의를 얻어 전자거래 인증서비스 등록신청을 대행하는 기능을 수행한다.

거래확인신청수단(221)은 전자거래관련사업자가 구매자와의 전자거래 발생시, 구매자의 전자서명용 비밀키로 전자서명된 구매정보에 대하여 전자거래관련사업자의 비밀키로 전자서명 후, 전자거래인증기관에 전자거래의 구매신청의 확인을 요청하는 기능을 수행한다.

전자거래인증기관 서버(230)는 상기 전자거래관련사업자 서버(220)의 고객에 대한 인증서비스 등록신청에 따라 전자서명용 비밀키, 공개키 쌍을 생성하고, 인증서를 발급하며, 생성된 전자서명용 비밀키를 암호화하여 전송하며, 암호화된 전자서명용 비밀키를 복호화할 수 있는 비밀번호를 고객등록시 지정한 전자우편주소로 발신하고, 상기 구매자 단말장치(210)로부터 상기 전자거래인증기관으로부터 인증서를 발급 받은 전자거래관련사업자 서버간의 전자거래 발생시, 전자상거래사업자 서버(220)의 거래확인신청수단(221)에서 구매자 및 전자거래관련사업자의 전자서명용 비밀키로 전자서명 된 구매정보가 전송되면 데이터센터 단위로 분산구축 된 디렉토리서버를 검색하여 구매자 및 전자거래관련사업자 인증서의 유효성을 확인하고 구매자 및 자거래관련사업자에게 전자거래 발생 및 거래내역에 대한 확인서를 발신하고 전자거래와 연계된 과금, 청구, 중계, 물류 등의 부가서비스를 진행시키는 시스템으로써, 부가서비스연동수단(231), 키 쌍 생성수단(232), 디렉토리관리수단(233), 인증서 발급수단(234), 전자거래확인수단(235) 및 인증서비스 연동수단(236)으로 이루어진다.

부가서비스연동수단(231)은 전자거래와 연계된 청구, 과금, 중계, 물류 등의 처리절차를 담당하는 부가서비스시스템(240)과의 연동 기능을 제공한다.

키 쌍 생성수단(232)은 구매자 및 전자거래사업자의 인증서 발급 요청에 따라 전자서명용 비밀키, 공개키 쌍을 생성하고 디렉토리서버에 저장하는 기능을 수행한다.

디렉토리관리수단(233)은 인증서를 저장 및 관리하고, 전자거래 단위의 거래 확인요청시 상대적인 가입자 경로를 기준으로 분산 구축된 디렉토리를 검색하여 인증서의 유효성을 확인하는 기능을 수행한다.

인증서발급수단(234)은 전자서명용 비밀키를 암호화하여 전송하고 암호화된 비밀키를 복호화 할 수 있는 비밀번호를 인증서비스 등록 시 지정한 전자우편주소로 발신하는 기능을 수행한다.

전자거래확인수단(235)은 전자거래 단위의 거래 확인요청 시 상대적인 가입자 경로를 기준으로 분산 구축된 디렉토리를 검색하여 인증서의 유효성을 확인하고 구매자 및 전자거래관련사업자에게 확인서를 발신하는 기능을 수행한다.

인증서비스연동수단(236)은 전자거래 단위의 인증서비스 제공을 위하여 데이터센터 단위로 분산구축된 인증시스템의 연동기능을 제공한다.

상술한 구성에 의거하여 각각의 데이터센터에 인증시스템을 분산구축하고 전자거래 단위의 인증서비스를 제공하는 절차에 대하여 상세히 설명하기로 한다.

먼저, 전자거래인증기관은 인증시스템(230)을 이용하여 상기 전자거래관련사업자의 서버(220)에 별도의 절차에 따른 인증서를 발급하고, 상기 전자거래관련사업자는 발급 받은 서버인증서와 구매자 단말장치(210)에서 생성한 세션키를 근간으로 전자거래관련사업자와 구매자의 단말장치간 보안채널을 설정한다.

상기 전자거래관련사업자는 구매자의 고객등록 및 갱신 처리과정에서 구매자의 동의하에 상기 전자거래인증기관에 구매자의 전자거래 인증서비스 등록신청을 수행한다.

상기 전자거래관련사업자 서버(220)의 인증등록 신청수단(221)의 요청에 따라 키 쌍의 생성수단(232)은 구매자의 전자서명용 비밀키, 공개키 쌍 및 인증서를 생성하여 디렉토리 서버에 저장하고, 생성된 구매자의 전자서명용 비밀키는 인증서 발급수단(234)에 의해 암호화되어 구매자에게 전송되고 이를 복호화 할 수 있는 비밀번호를 구매자가 인증서비스 등록신청 시 지정한 전자우편주소로 발신된다.

구매자는 구매자단말장치(210)에 전자거래인증기관의 인증시스템(230)으로부터 전송된 구매자의 암호화된 전자서명용 비밀키를 저장하며, 지정한 전자우편주소로 발신된 비밀번호를 이용하여 비밀키를 복호화 하고 구매자 단말장치 내에 인증서를 저장한다.

전자거래인증기관의 인증서를 발급받은 구매자와 데이터센터내.외의 전자거래인증기관의 서버인증서를 발급받은 임의의 전자거래관련사업자간의 전자거래발생 시, 구매자의 전자서명 후 전자거래관련사업자 서버에 주문내역을 전송하면 전자거래관련사업자의 거래확인신청수단(221)은 주문내역에 전자서명 후, 전자거

러인증기관의 거래확인수단(235)에 확인을 요청한다.

전자거래인증기관의 거래확인수단(235)은 인증서비스연동수단(236)을 통하여 데이터센터 단위로 분산구축된 디렉토리서버를 검색하여 구매자 및 전자거래관련사업자 인증서의 유효성을 확인하고 전자거래인증기관의 전자서명 후, 구매자 및 전자거래관련사업자에게 확인서를 전송한다.

전자거래인증기관의 확인을 근간으로 부가서비스연동수단(236)은 전자거래와 연계된 과금, 청구, 중개, 물류 등의 관련절차를 진행한다.

도면과 명세서는 단지 본 발명의 예시적인 것으로서, 이는 단지 본 발명을 설명하기 위한 목적에서 사용된 것이지 의미 한정이나 특허청구범위에 기재된 본 발명의 범위를 제한하기 위하여 사용된 것은 아니다. 그러므로, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

발명의 요약

본 발명에 의하면, 전자거래 단위의 인증시스템 개발하여 전자거래의 안전성 및 신뢰성을 제공하여 전체 전자거래시장의 성장에 기여하고, 전자거래시장에서의 구매자 및 판매자의 전자거래에 연계된 인증서 발급 절차의 개발로 광범한 PKI의 구축이 용이하며, 가상적인 전자거래시장의 중심이 되는 데이터센터 단위로 인증시스템을 분산구축 함으로써 안정적인 인증서비스 제공과 인증서비스의 효율적인 운용이 가능하다.

또한, 본 발명에서 제시된 구매자와 전자거래관련사업자 간의 전자거래 단위의 인증서비스 모델은 전자거래관련사업자간의 전자거래 단위의 인증서비스 제공에도 동일하게 적용가능하다.

(57) 청구의 범위

청구항 1

적어도 하나의 전자거래관련사업자와 전자거래인증기관을 포함하는 데이터센터 단위로 분산된 인증시스템에 있어서,

상기 전자상거래관련사업자에 인증서를 발급하는 전자거래인증기관 서버; 및

상기 발급 받은 서버인증서와 구매자 단말장치에서 생성한 세션키를 근간으로 구매자 단말장치와의 보안채널을 설정하고, 구매자의 고객등록 및 갱신신청 처리과정에서 구매자의 동의하에 전자거래인증서비스 등록을 신청하는 전자거래관련사업자 서버를 포함하고,

상기 전자거래인증기관 서버는

구매자의 신청에 따라 구매자의 전자서명용 비밀키,공개키쌍을 생성하고 구매자의 전자서명용 비밀키를 암호화하여 전송하고, 구매자에게 인증서를 발급 및 저장하고, 암호화된 구매자의 전자서명용 비밀키를 복호화할 수 있는 비밀번호를 구매자가 등록신청시 지정한 전자우편주소로 발신하며 구매자가 단말장치에 인증서를 저장할 수 있게 함을 특징으로 하는 데이터 센터의 전자거래 인증시스템.

청구항 2

제1항에 있어서,

상기 구매자와 상기 전자거래인증기관의 서버인증서를 발급받은 데이터센터내 외의 임의의 전자거래관련사업자간의 전자거래 발생시,

상기 전자거래관련사업자 서버는

상기 구매자가 전자서명한 구매신청에 대한 확인을 전자거래사업자의 전자서명 후, 상기 전자거래인증기관의 서버에 요청하도록 프로그램되고,

상기 전자거래인증기관 서버는

데이터센터단위로 분산구축된 디렉토리서버를 검색하여 구매자 및 전자거래관련사업자 인증서의 유효성을 확인하고 인증기관의 전자서명 후, 상기 구매자 및 전자거래관련사업자의 거래발생 및 거래내역에 대한 확인서를 발급하도록 프로그램되고, 이를 근거로 전자거래와 연계된 과금, 청구, 중개, 물류 등의 관련절차를 진행할 수 있게 하는 프로그램됨을 특징으로 하는 데이터 센터의 전자거래 인증시스템.

청구항 3

제1항에 있어서, 상기 전자거래관련사업자 서버는

상기 전자거래인증기관 서버로부터 발급받은 서버인증서를 근간으로 구매자 단말장치와 보안채널을 설정하고, 구매자의 고객등록 및 갱신신청 과정에서 구매자의 동의를 얻어 전자거래 인증서비스 등록신청을 대행하는 인증등록신청수단; 및

상기 전자거래관련사업자가 구매자와의 전자거래 발생시, 구매자의 전자서명용 비밀키로 전자서명된 구매정보에 대하여 전자거래관련사업자의 비밀키로 전자서명 후, 전자거래인증기관에 전자거래의 구매신청의 확인을 요청하는 거래확인신청수단을 포함함을 특징으로 하는 데이터 센터의 전자거래 인증시스템.

청구항 4

제1항에 있어서, 상기 전자거래인증기관의 서버는

상기 전자거래관련사업자의 서버에 소정의 절차에 따라 인증서를 발급하는 인증서 발급수단;

상기 전자거래인증기관의 서버에서 등록신청에 따라 구매자의 전자서명용 비밀키, 공개키쌍을 생성하는 키 쌍 생성수단;

상기 인증서를 저장 및 관리하고, 전자거래 단위의 거래 확인요청시 상대적인 가입자 경로를 기준으로 분산 구축하는 디렉토리관리수단;

상기 전자거래 단위의 거래 확인요청시 상대적인 가입자 경로를 기준으로 분산 구축된 디렉토리를 검색하여 인증서의 유효성을 확인하고 구매자 및 전자거래관련사업자에게 확인서를 발신하는 전자거래확인수단;

상기 전자거래인증기관의 서버에서 데이터센터 단위로 분산구축된 디렉토리서버를 검색하여 상기 구매자 및 전자거래관련사업자 인증서의 유효성을 확인하고 전자거래인증기관의 전자서명 후, 구매자 및 전자거래관련사업자에게 거래발생 및 거래내역에 대한 확인서를 발급하고, 이를 근거로 전자거래와 연계된 과금, 청구, 중개, 결류 등의 관련 절차를 진행하는 부가서비스연동수단; 및

상기 전자거래 단위의 인증서비스 제공을 위하여 데이터 센터 단위로 분산구축된 인증시스템간에 연동하는 인증서비스연동수단을 포함함을 특징으로 하는 데이터 센터의 전자거래 인증시스템.

청구항 5

제4항에 있어서, 상기 인증서발급수단은

상기 전자거래인증기관의 서버에서 생성된 구매자의 전자서명용 비밀키를 암호화하여 전송하고 암호화된 비밀키를 복호화 할 수 있는 비밀번호를 인증서비스 등록시 지정한 전자우편주소로 발신하는 기능을 수행함을 특징으로 하는 데이터 센터의 전자거래 인증시스템.

청구항 6

데이터센터 단위로 인증시스템을 분산 구축하고 전자거래 단위의 인증서비스 제공방법에 있어서,

(a)전자거래관련사업자 서버에 접속한 구매자 단말장치에서 생성한 세션키를 근간으로 상기 전자거래관련사업자 서버와 상기 구매자 단말장치간의 보안채널을 설정하는 단계;

(b)상기 전자거래관련사업자 서버가 구매자의 고객등록 및 갱신 처리과정에서 구매자의 동의를 얻어 전자거래인증기관에 인증서비스 등록을 신청하는 단계;

(c)상기 구매자의 인증서비스 등록신청에 따라 상기 전자거래인증기관 서버는 구매자의 전자서명용 비밀키,공개키 쌍을 생성하고, 생성된 가입자의 전자서명용 비밀키는 암호화하여 구매자에게 전송하며, 구매자의 인증서를 발급 및 저장하고, 암호화된 구매자의 전자서명용 비밀키를 복호화할 수 있는 비밀번호를 구매자가 인증서비스 등록시 지정한 전자우편주소로 전송하는 단계;

(d)상기 구매자 단말장치에 전자거래인증기관 서버로부터 전송된 구매자의 암호화된 전자서명 비밀키를 저장하며, 지정한 전자우편주소로 발신된 비밀번호를 복호화하고 구매자의 단말장치내에 저장하는 단계;

(e)상기 전자거래인증기관 서버로부터 인증서를 발급받은 구매자와 데이터센터내,외의 전자거래인증기관의 서버인증서를 발급받은 임의의 전자거래관련사업자간의 전자거래발생시, 구매자의 전자서명 후 상기 전자거래관련사업자 서버에 주문내역을 전송하는 단계;

(f)상기 전자거래관련사업자 서버는 상기 구매자 단말장치로부터 전송된 주문내역에 대하여 전자서명 후, 전자거래인증기관 서버에 확인을 요청하는 단계;

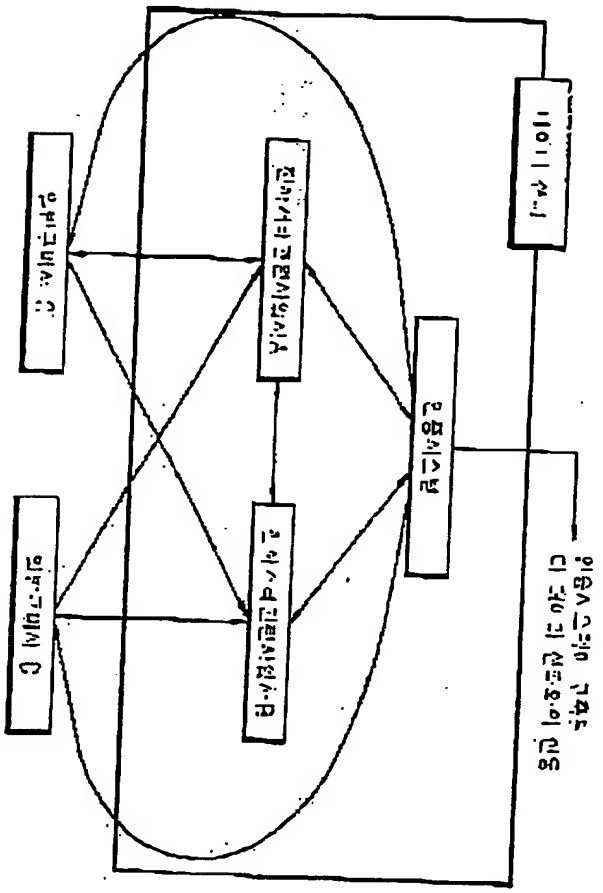
(g)상기 전자거래인증기관 서버는 데이터센터 단위로 분산구축된 디렉토리서버를 검색하여 구매자 및 전자거래관련사업자 인증서의 유효성을 확인하고 전자거래인증기관의 전자서명 후, 상기 구매자 단말장치 및 전자거래관련사업자 서버에 확인서를 전송하는 단계; 및

(h)상기 전자거래인증기관 서버의 확인을 근간으로 전자거래와 연계된 과금, 청구, 중개, 결류 등의 관련 절차를 진행하는 단계를 포함함을 특징으로 하는 데이터 센터의 전자거래 인증서비스 제공방법.

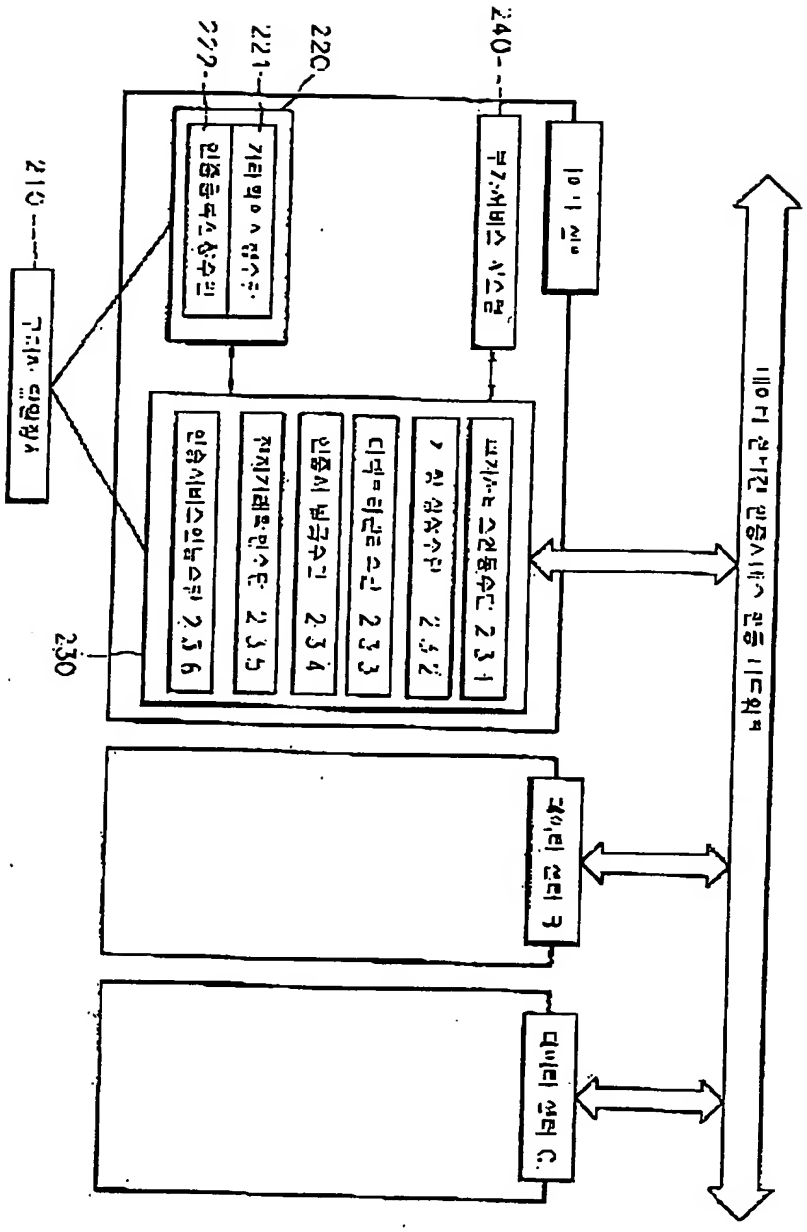
도면

특2000-0024217

도면1



도면2


210
220
221
222
240
230
231
232
233
234
235
236
인터페이스 블록
데이터 버스
데이터 버스 B
데이터 버스 C